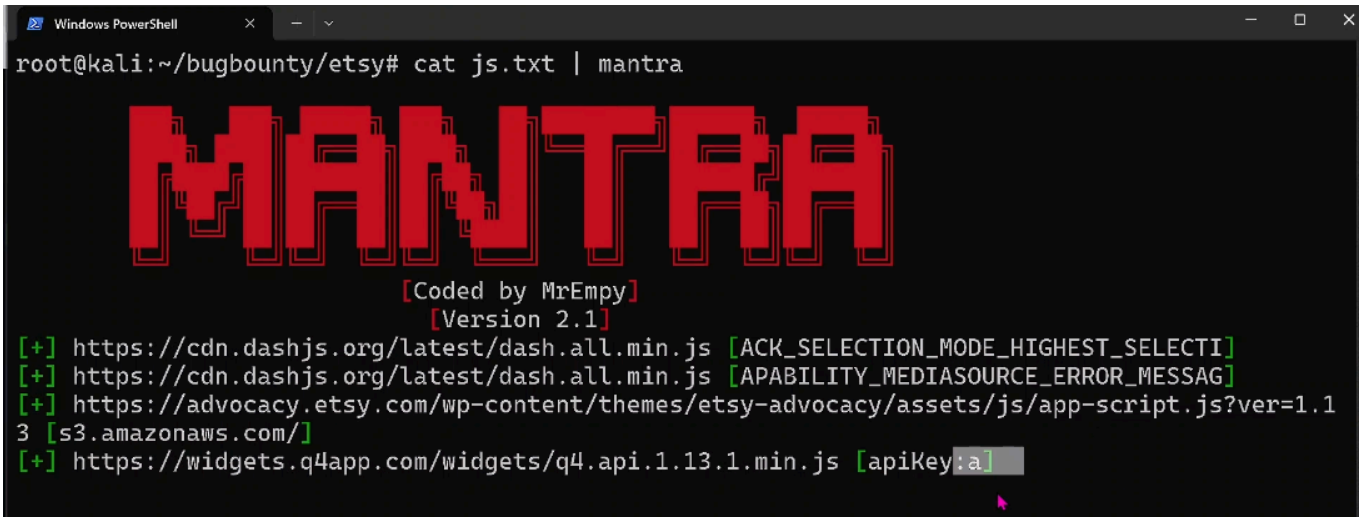
JavaScript Analysis

- wayback
- gospider
- katana
  => allurls.txt
  اول حاجه لازم تكون مجمه كل urls

1- Use Mantra => for api keys



- الاداه بتشتغل زي كدا
- شكل ال api بيبقي مكان الـ api كدا apikey: api

- لازم تنزل الملفات عندك الاول علي السيرفر عن طريق curl او wget مع for loop
  Use jsluice => for secrets and urls => jsluice urls player.js -2
  jsluice secrets player.js
  for i in $(ls);do jsluice secrets $i;done

```
root@kali:~/bugbounty/etsy/js#  for i in `cat js.txt`;do wget $i;done
```

- زي كدا
- لازم تعمل فولدر تحطهم فيه وتبقي فيه
- ```
  for i in $(ls);do jsluice secrets $i;done
  ```
- لو عايز تعملها ع كلو مره واحده

  ```

3- Use nuclei => nuclei-tempates/http/exposures/
nuclei -l js.txt -t /root/nuclei-templates/http/exposures/ -mhe 4

- حاول تبعد عن ملفات wp علشان الثغرات بتبقي متصلحه

4- analyze the code with js beaty in visual studio code

- بتنزل beautifiy extention
- عشان تشغله ctrl+shift+p